

⑫ 公開特許公報(A)

平1-161469

⑪ Int. Cl.⁴
G 06 F 15/06識別記号
3 2 0庁内整理番号
A-7343-5B

⑬ 公開 平成1年(1989)6月26日

審査請求 未請求 請求項の数 3 (全9頁)

⑭ 発明の名称 保証オンチップPROMを有する単一チップ・マイクロプロセッサ

⑮ 特 願 昭63-268370

⑯ 出 願 昭63(1988)10月26日

優先権主張 ⑰ 1987年11月3日 ⑱ 米国(US) ⑲ 116,607

⑳ 発 明 者 ジェフリー・ブイ・マ アメリカ合衆国テキサス州 78619、ドリフトウッド、エ
イヤーズ ルダーヒル・ロード 134㉑ 出 願 人 モトローラ・インコー アメリカ合衆国イリノイ州 60196、シャンバーグ、イー
ボレーテッド スト・アルゴンクイン・ロード 1303

㉒ 代 理 人 弁理士 池内 義明

明 細 書

1. 発明の名称

保証オンチップPROMを有する
単一チップ・マイクロプロセッサ

2. 特許請求の範囲

1. 単一半導体チップ上のマイクロプロセッサ
であって、

半固定記憶装置(PROM)と、

該PROMに含まれている情報を処理する処理
手段と、前記マイクロプロセッサの外部の源から受取っ
た入力信号に応じて、前記処理手段により提供さ
れた前記PROM情報にプログラムするプログラ
ミング手段と、を具備して成ることを特徴とするマイクロプロセ
ッサ。2. 処理手段は前記外部の源に出力信号を供給
して前記PROMにプログラムすべき前記情報が
提供されたことを示す特許請求の範囲第1項に記

載のマイクロプロセッサ。

3. 処理手段はデータ・ラッチおよびアドレス
・ラッチが前記データおよびアドレスをそれぞれ
ラッチして後第1の制御信号を発生し、プログラ
ミング手段は、前記入力信号と前記第1の制御信号とに応じて、
プログラム・イネーブル信号を発生する第1の論
理手段と、前記プログラム・イネーブル信号に応じて、前
記データ・ラッチ内のデータを前記PROMの前
記アドレス・ラッチ内のアドレスにプログラムす
る手段と、を具備している特許請求の範囲第1項に記載のマ
イクロプロセッサ。

3. 発明の詳細な説明

〔産業上の利用分野〕

本発明は、一般に同一半導体チップ上にプログ
ラム可能ROMまたは半固定記憶装置(PROM)
を有するマイクロプロセッサに関し、更に詳細に
は、保証(secure)PROMを有するマイクロプロ

セッサに関する。

〔従来の技術〕

1976年、インテル社は同一半導体チップ上に半固定記憶装置(PROM)を有する最初のマイクロプロセッサを公表した。この初期の製品、8748、においては、PROMは消去可能半固定(EPRM)の形態のものであり、EPRMをオンチップ・プロセッサと完全に独立にプログラムするには従来の形態の外部PROMプログラマが必要であった。このプロセッサについてはBlume に対して発行された米国特許第 4,153,933号に図示され記述されている。1976年11月25日発行のエレクトロニクス誌には、「単一チップ8ビット・マイクロコンピュータが計算機形式のプロセッサと強力なマルチチップ・プロセッサとの間隙を埋める」と題する論文で、8748が更に、「紫外線でクリアすることにより変更することができると共に通常の方法で電氣的にプログラムし直すことができる」2708形式のEPRMを備えているものとして説明されている。(p. 100、

チップ内に「動かされる(moved)」(第5図と第7図の16~34行を参照)。こうして特別のI/O命令が実行されて「プログラミング」ラッチP(第3図の113)がプログラミング信号PGをプログラミング回路に出力するようにセットされる。(第7図の49行近くの「OUTLP, A」マイクロ命令を参照)。適切なプログラム期間、たとえば、50ミリ秒だけ待ちループを実行してから(第4図と第5図および第7図の50~51行付近の「DJNZ Rx, Comp t」マイクロ命令を参照)、別の特別I/O命令が実行されてPラッチをリセットする。(第7図52行あたりの「OUTPA」マイクロ命令を参照)。

〔発明が解決しようとする課題〕

この「自己プログラミング」形式の多数の他のマイクロプロセッサが近年紹介されているが、すべて外部プログラミング機構か内部プログラミング機構かを利用している。しかしながら、両機構ともある用途においては欠点を有している。たとえば、いわゆる「スマートカード」の用途では、

パラグラフの最初の文は左欄の下から始まっている。)

1979年、モトローラ社はオンチップ・プロセッサの制御のもとに完全にプログラムすることができるEPRMを備えた最初のマイクロプロセッサを発表した。このマイクロプロセッサMC68701は、現在放棄されているが米国特許出願第912,183号として継続中の米国特許出願第047,674号に図示され説明されている。

Ugon に対して発行された米国特許第 4,382,279号には、オンチップ修正可能(modifiable)記憶装置を備えた単一チップ・マイクロプロセッサが開示されている。Ugonの特許では、Blume と異なり、EPRMはオンチップ・プロセッサの制御のもとに書き込み可能である。制御記憶装置と修正すべき記憶装置とに同時にアクセスすることができるように、アドレスとデータのラッチが二重に設けられている。制御記憶装置の外で実行するプログラムの制御のもとで、修正すべき記憶装置の部分の特定のアドレスに書込まれるデータがこれら

オンチップPROMの保証(security)が最高に重要である。このような用途では、内部プログラミング・モードが望ましく、それによりプログラミング機構はオンチップ・プロセッサがすべての保証試験に合格したことを確認した場合に限り使用可能となる。しかしながら、現在利用できるマイクロプロセッサで動作において全体として「フェールセーフ」になっているものはなく、一般に、ある悪条件下で「粗野になり(go wild)」、無秩序なコードを実行することになる。このような事態において、このような無秩序なコードを実行した直接の結果として、プロセッサがオンチップPROMプログラミング回路を不注意にも使用可能としてオンチップPROM内の重要なデータの保証を傷つけるという可能性は絶無ではない。この可能性を最小限にするため各種インターロックや「デッドマン」タイマ機構が提案されているが、この可能性を完全に除去する手順は発明されていない。

全般的に関連する先行技術は次の米国特許に図

示され説明されている。

Check, Jr. 等に対して発行された米国特許第 3,978,457号では、CPUと郵便会計情報を格納する持久記憶装置とを備えたマイクロコンピュータ化電子式郵便料金メータ・システムを開示している。このcheckの特許では、持久記憶装置は電池バックアップのシフトレジスタの形態として開示されているので、これへの書込みは非常に容易である。すなわち、特別なハードウェアあるいは書込みシーケンスは不要である。

Fletcher, III等に対して発行された米国特許第 4,018,565号では、マイクロプロセッサとオペレータ入力パラメータを格納するリードモストリ・メモリ(read-mostly memory)とを備えた自動プロセス滴定システムを開示している。この特許では、リードモストリ・メモリは電気的に変改可能なものとして開示されており、かつマイクロプロセッサには「複雑な読み書き手順」を制御する特別な読み書きサブルーチンが設けられている。

Weisgerber等に対して発行された米国特許第

4,107,785号ではマイクロプロセッサを使用するプログラム可能制御装置を開示している。同じあるいは同様なプログラム可能制御装置がHillerに対して発行された米国特許第 4,093,998号に開示されている。

従って、本発明の目的は、外部エンティティの許可ある場合にのみオンチップ・プロセッサが提供した情報でプログラムすることができるオンチップPROMを備えた単一チップマイクロプロセッサを提供することである。

本発明の他の目的は、外部エンティティがプログラミング・イネーブル信号を提供しなければオンチップ・プロセッサによりオンチップPROMをプログラムできないようにする保証インターロック機構を有する単一チップ・マイクロプロセッサを提供することである。

〔課題を解決するための手段〕

これらおよび他の目的は、半固定記憶装置(PROM)、該PROMに入っている情報を処理するプロセッサ、および前記マイクロプロセッサの

4,045,660号では、CPUと自動整列データを格納する持久記憶装置とを備えた、停電後機械要素を所定の位置に自動的に整列し直す方法と装置とが開示されている。

Foudosに対して発行された米国特許第

4,053,735号では、マイクロプロセッサと転送コードおよび勘定残高情報を格納する持久記憶装置とを備えた融資チェック・コンピュータベース銀行クレジット支払いシステムを開示している。この特許では、持久記憶装置は電池バックアップRAMの形態のものとして開示されているので、その書込みは非常に容易である。すなわち、特別なハードウェアや書込みシーケンスを必要としない。

Soulsby 等に対して発行された米国特許第

4,078,259号では、外部の場所(locations)で論理状態を監視するシステムを備えたプログラム可能制御装置を開示している。同じあるいは同様なプログラム可能制御装置がHillerに対して発行された米国特許第 4,093,998号に開示されている。

Seipp に対して発行された米国特許第

外部の源から受取った入力信号にตอบสนองして、前記PROMに前記処理手段により提供された情報をプログラミングするプログラミング回路を具備する、単一半導体チップ上のマイクロプロセッサにより達成される。

〔実施例〕

第1図に示すのは一般に、単一半導体チップ上に、プロセッサ(CPU)12と、紫外線(UV)により消去可能な半固定記憶装置(EPROM)か電気的に消去可能な半固定記憶装置(EEPROM)形式かの半固定記憶装置(PROM)14と、CPU12が提供した情報を、外部データ・プロセッサのような外部エンティティ(図示せず)から、外部インタフェース・ピン18を経てSTART信号を受取ることに応じてのみPROM14に書込むプログラミング制御装置16とを具備するマイクロプロセッサ10である。通常動作では、CPU12はPROM14に格納されている情報を処理し、アドレスバス20を経由してアドレスを発し、PROM14が提供するデータを

データバス22を経由して受取る。プログラミング制御装置16が発した読取り(R)信号に応じて、アドレス・マルチプレクサ(MUX)24はアドレスバス20を直接PROM14に結合し、一方データ・マルチプレクサ(MUX)26はデータ・バス22を直接PROM14に結合する。

PROMプログラミング動作では、CPU12はPROM14に書込むべきデータをデータバス22を経由して提供し、そのデータを書込むべきアドレスをアドレスバス20を経由して提供する。同時に、CPU12はPROM書込み(PW)信号を提供する。PW信号に応じて、1組のデータラッチ28がCPU12によりデータバス22に供給されたデータをラッチし、一方1組のアドレスラッチ30がCPU12によりアドレスバス20に供給されたアドレスをラッチする。PW信号を検出すると、プログラミング制御装置16はR信号を無効とし、相補書込み(W)信号を効果的に発生する。W信号に応じて、アドレス・マルチプレクサ(MUX)24はアドレスラッチ30

の出力をPROM14に結合し、データ・マルチプレクサ(MUX)26はデータラッチ28の出力をPROM14に結合する。実質上同時に、プログラミング制御装置16はARM信号を発生する。この点で、CPU12は他の任務に自由に進めるが、プログラミング・サイクルは始まっていない。

第1図に示す好ましい実施例では、プログラミング・サイクルはプログラミング制御装置16がSTART信号をマイクロプロセッサ10の外部にある源(図示せず)から外部インタフェース・ピン18を経由して受取ったことに応じてのみ開始することができる。特定の用途により、START信号は外部の源(図示せず)から連続的に提供することができ、あるいはCPU12が特別な情報を別の外部インタフェース・ピン32を経由して供給したことに応じてのみ提供することができる。いずれにしても、START信号はエッジ・センシティブ、レベル・センシティブ、あるいはコンテンツ・センシティブの場合があり、適切

な外部状態検出回路34が設けられていてSTART信号を検出し、内部対応START信号を発する。

プログラミング制御装置16により供給されるARM信号と検出器34により供給される内部START信号との双方を受取ったことに応じて、ANDゲート36はENABLE信号をプログラミング電圧発生器38に供給し、PROM14のプログラミング・サイクルを開始する。検出器34により供給される内部START信号を検出したことに応じて、プログラミング制御装置16はPROM14が必要とするプログラミング時間に適応するように選定されたタイミング・シーケンスを開始する。プログラミング期間の終りに、プログラミング制御装置16はARM信号を無効とし、ANDゲート36にENABLE信号を無効にさせ、発生器38によるPROM14へのプログラミング電圧の印加を終了する。実質的に同時に、プログラミング制御装置16はDONE信号を発生してCPU12にPROM14のプログ

rammingが完了したことを知らせることができる。

プログラミング・サイクル中、CPU12は、DONE信号により中断されるまで別の任務(tasks)を行うこと、DONE信号待ちを循環させること、あるいはDONE信号で「起こされる」のを持って「眠る」ことができる。いずれの場合でも、DONE信号に応じて、CPU12は今ちょうどPROM14に書き込まれた情報を読取って、他の任務に進む前に、望むならばその正確さを確認することができる。望むならば、CPU12はプログラミング制御装置16にDONE信号を発生するよう要求するのではなく単にARM信号を監視することができる。

第2図に示す別の実施例では、外部インタフェース・ピン18'はプログラミング用外部電圧源(図示せず)を電圧源選択スイッチ40により発生器38に結合するのにも使用される。1対の電圧シフトバッファ34'と34''とが外部プログラミング電圧 V_{pp} の有無を検出し、 V_{pp} が存在すれば内部START信号を発生する。この場合、

バッファ34' と34" とはピン18' にかかる電圧がグラウンド電圧 V_{SS} と通常供給電圧 V_{DD} の間のある所定電圧より高くなったとき、スイッチ40が内部チャージ・ポンプ42からプログラミング電圧を発生して、内部START信号を発生するように構成することもできる。

第3図に示す実施例においては、別の V_{PP} ピン44が設けられており、外部インタフェース・ピン18" は双方向性であり、その方向は一般的なデータ方向レジスタ46で決められるようになっている。ANDゲート48はデータ方向レジスタ46が入力状態になっているときCPU12がピン18" を経由して出力信号を供給しないようにしている。ANDゲート48はまたプログラミング制御装置16がARM信号を発生しているときCPU12がバッファ34' および34" を経由してそれ自身START信号を発生することがないようにしている。この構成において、CPU12は、

第1に、データ方向レジスタ46を出力状態に

セットし、望むならば、プログラミングを次のクロック・サイクルで開始することができるということを示す信号を外部源（図示せず）に対して出力する、

第2に、PW信号を使用して適切なアドレスとデータとの情報をそれぞれラッチ30および28にラッチする、

第3に、データ方向レジスタ46を入力状態にセットして外部源（図示せず）がSTART信号を発生することができるようにする、

最後に、プログラミング・サイクルが完了するまで待つ、

ように容易にプログラムすることができる。

START信号はポート読取りデータ経路を経てCPU12に見えるようになっているから、CPU12は、START信号を受取るかあるいは外部源（図示せず）が知らせを受けてから妥当な時間が経過するかするまで循環(loop)するように、そして外部源（図示せず）が知らせを受けてから妥当な時間が経過したとき、プログラミングが承

認されなかったものと判断し、単に適切な例外ルーチンか別の意味ある任務かのいずれか適切な方に進むだけにするように、容易にプログラムすることができる。望むならば、このような構成は第1図および図2図に示す実施例に設けることもできる。

第4図に示す実施例においては、外部インタフェース・ピン18'" を、CPU12が第3図の場合のように通常の双方向ポートとして、あるいは一般的な直列通信インタフェース(SCI)50が半二重直列通信ポートとして、使用することができる。CPU12がアドレスバス20およびデータバス22を經由して送信オペランドを送信データレジスタ52にロードしたことに応じて、SCI50は送信(XMIT)ON信号を発生し、マルチプレクサ54にビットシリアル(bit-serial)送信データ(TXD)信号をANDゲート48（これはORゲート56を介してイネーブルされる）を経てピン18'" に結合できるようにさせる。この形態では、SCI50をCPU12

が外部プログラミング制御装置（図示せず）にPROM14がプログラミング可能な感勢にあるという適切な信号を送信するのに使用することができる。外部制御装置（図示せず）の返答をバッファ34' と34" を經由してビットシリアル受信データ(RXD)信号として受信したことに応じて、SCI50は受信オペランドを受信データレジスタ58にロードする。受信データレジスタ58が満杯であるか満杯になる手前であるかを示す割込み(INT)信号をSCI50から受信したことに応じて、CPU12は特別な値をキーレジスタ60にロードする。受信データレジスタ58に入っているオペランドがキーレジスタ60の中の特別な値と同じであることを検出したら、比較器62はSTART信号を発生し、プログラミング・サイクルを開始する。望むなら、外部制御装置（図示せず）がCPU12により供給される対応する特別な値の対応する連鎖に合致するオペランドの連鎖を発生しなくてはならなくなるように別の論理を追加することができる。同様に、

キーレジスタ60と比較器62とは、望むならば、除外して、たとえば、受信データレジスタ58のオペランドの所定ビットが「セット」されている場合START信号を発生するように非常に簡単な論理と置換えることができる。CPU12は返答を外部制御装置（図示せず）から受取ると常にINT信号により割込まれ、受信データレジスタ58の中のオペランドをアドレスバス20およびデータバス22を経由して容易に読取ることができるから、CPU12は外部制御装置（図示せず）の判断を検知することができる。

第5図に示す簡略形態では、単純なフリップフロップ64が発生器38を制御してPROM14のプログラミングを可能にしている。アドレスおよびデータを、PW信号により、それぞれアドレスラッチ30およびデータラッチ28にラッチしてから、CPU12は適切な信号をピン18を経由して外部制御装置（図示せず）に供給する、その直後あるいはある所定の遅れ期間の後、CPU12は単極双投（SPDT）スイッチ66を作動

事象はCPU12に割込ませる、または「目を覚まさせる」のにも使用することができるから、これによりフリップフロップ64をクリアすることができる。もちろん、発生器38は、望むなら、PROMのプログラミングが完了したときフリップフロップ64を自動的にクリアするように「セルフタイミング」となるように構成することができる。本発明について好ましい実施例およびそのいくつかの修正案に関して説明してきたが、その他の変更案および修正案を本発明の精神および範囲を逸脱することなくこのようなあらゆる実施例に関して行うことができる。一般に、他の各種技法を使用して外部制御装置（図示せず）から受取ったSTART信号が正しいことを確認することができる。たとえば、外部インタフェース・ピン18は、直接にあるいはスイッチ66を介して、エッジ・センシティブ・カウンタ（図示せず）に結合することができるのでSTART信号は外部制御装置（図示せず）が所定数の信号「エッジ」を発生する場合に限り発生する。ただし、このよ

うしてピン18を直接フリップフロップ64のセット（S）入力に結合させる。外部制御装置（図示せず）からの次の入力パルスはフリップフロップ64をセットしてプログラミング・サイクルを開始する。フリップフロップ64がセットされたことを検出したら、CPU12はスイッチ66を解除してフリップフロップ64をピン18から切離す。この形態では、CPU12はスイッチ66をフリップフロップ64のS入力にアクセスできるように構成することはできない。別の多数の方法のいずれかによりプログラミング・サイクルを終結させることができる。たとえば、フリップフロップ64がセットされたことを検出してから適切な時間の後に、CPU12はフリップフロップ64のクリア（C）入力にクリア信号を発生することができる。適切な自律タイマ68を利用できる場合には、CPU12をフリップフロップ64がセットされたとき、タイマ68を「セットアップ」しかつ始動させ、時間が来たらフリップフロップ64をクリアさせることができる。時間経過

うなすべての形態では、START信号は所定の用途および所定の保証レベルに適切なエッジ・センシティブ、レベル・センシティブ、あるいはコンテンツ・センシティブの各判定基準に合致することになる。最小限度の保証を必要とするある用途では、システム設計者は信号経路を、直接的あるいは間接的に、第1図のピン32のような、CPU12の通常の出力か入出力ピンから外部インタフェース・ピン18まで設けるようにすることができるので、CPU12は、事実、START信号を自身で発生することができる。同様に、CPU12はARM信号をプログラム制御装置16ではなくANDゲート36に直接供給するように構成することができる。この後者の形態では、CPU12は好ましくはあらゆるタイミングを規制することもできる。

〔発明の効果〕

以上説明したように、本発明により外部エンティティの許可ある場合にのみオンチップ・プロセッサが提供した情報でプログラムすることができ

るオンチップPROMを備えた単一チップ・マイクロプロセッサが提供される。

4. 図面の簡単な説明

第1図は、本発明に従ってのみプログラムすることができる、オンチップPROMを備えた単一チップ・マイクロプロセッサのブロック回路図である。

第2図は、第1図に示すマイクロプロセッサの一修正形態を示すブロック回路図である。

第3図は、第1図に示すマイクロプロセッサの別の修正形態を示すブロック回路図である。

第4図は、第1図に示すマイクロプロセッサの他の修正形態を示すブロック回路図である。

第5図は、第1図に示すマイクロプロセッサの更に他の修正形態を示すブロック回路図である。

26…データ・マルチプレクサ、

28…データ・ラッチ、

30…アドレス・ラッチ。

特許出願人 モトローラ・インコーポレーテッド
代理人 弁理士 池内 毅 明

12…CPU、

14…半固定記憶装置(PROM)、

16…プログラミング制御装置、

24…アドレス・マルチプレクサ、

FIG. 1

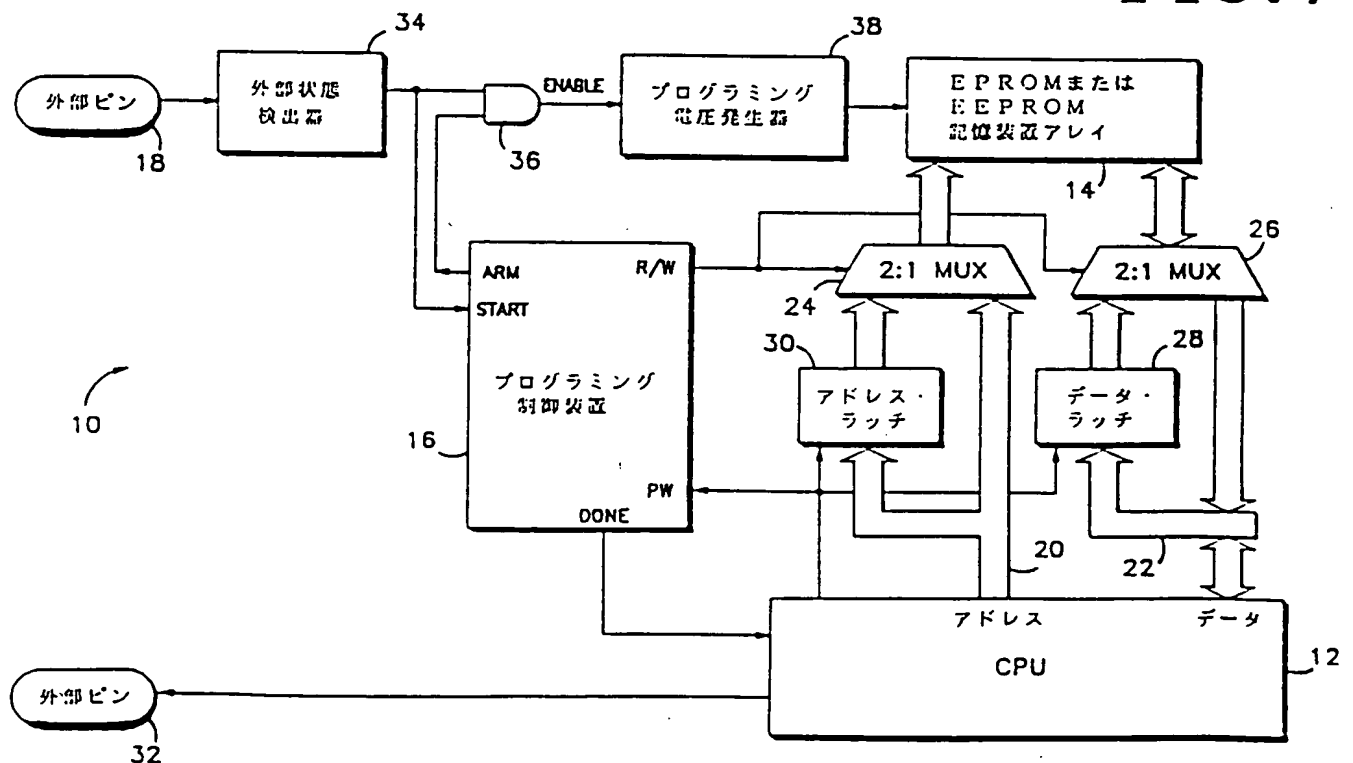


FIG. 2

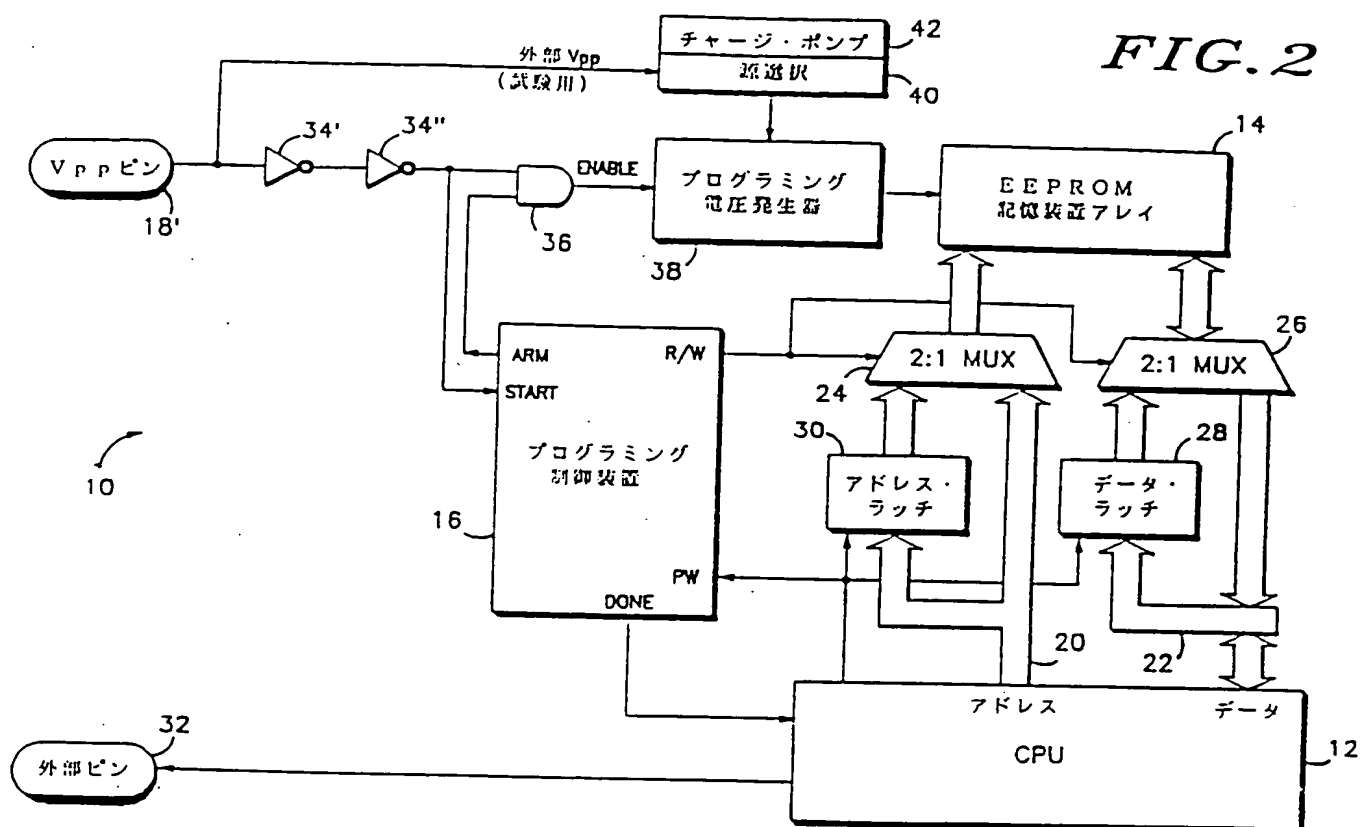


FIG. 3

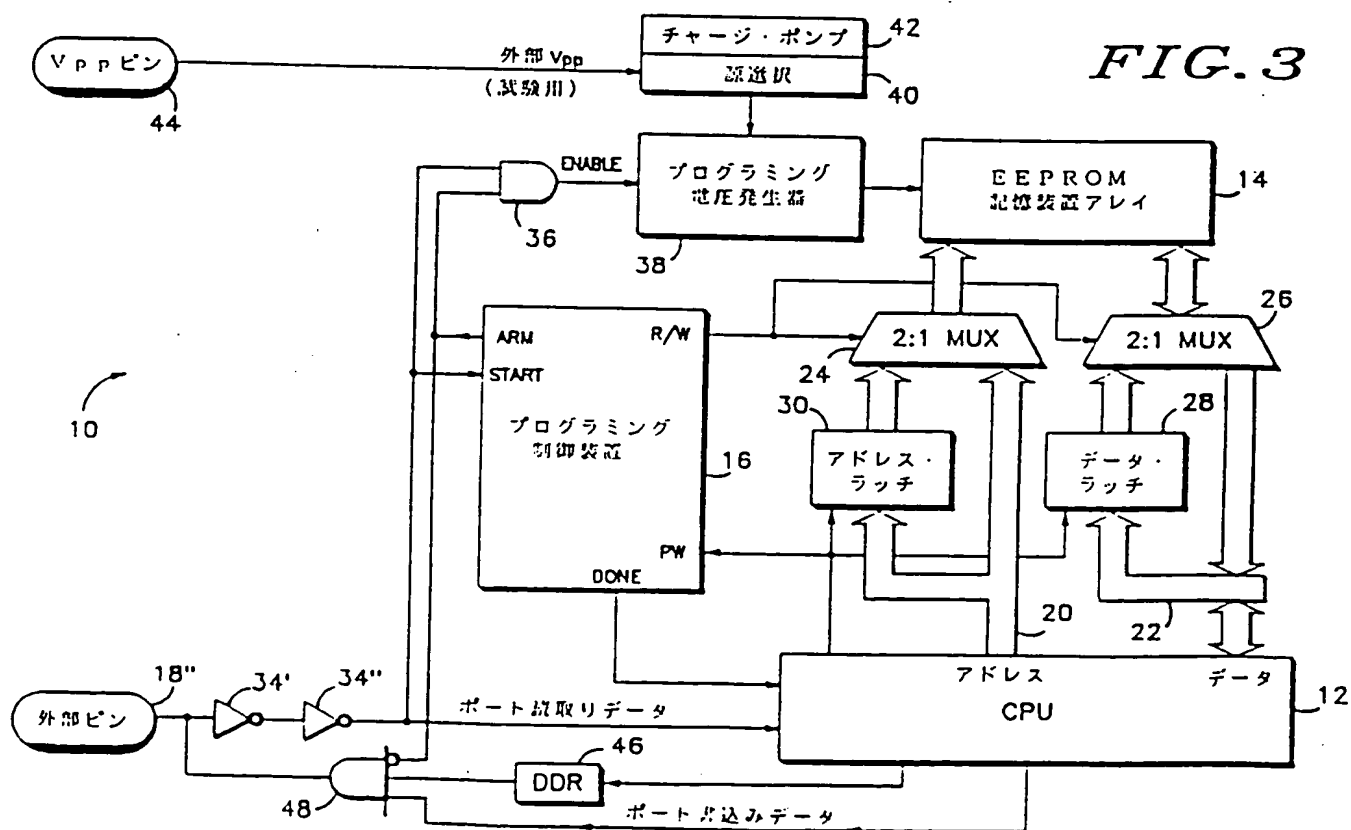


FIG. 4

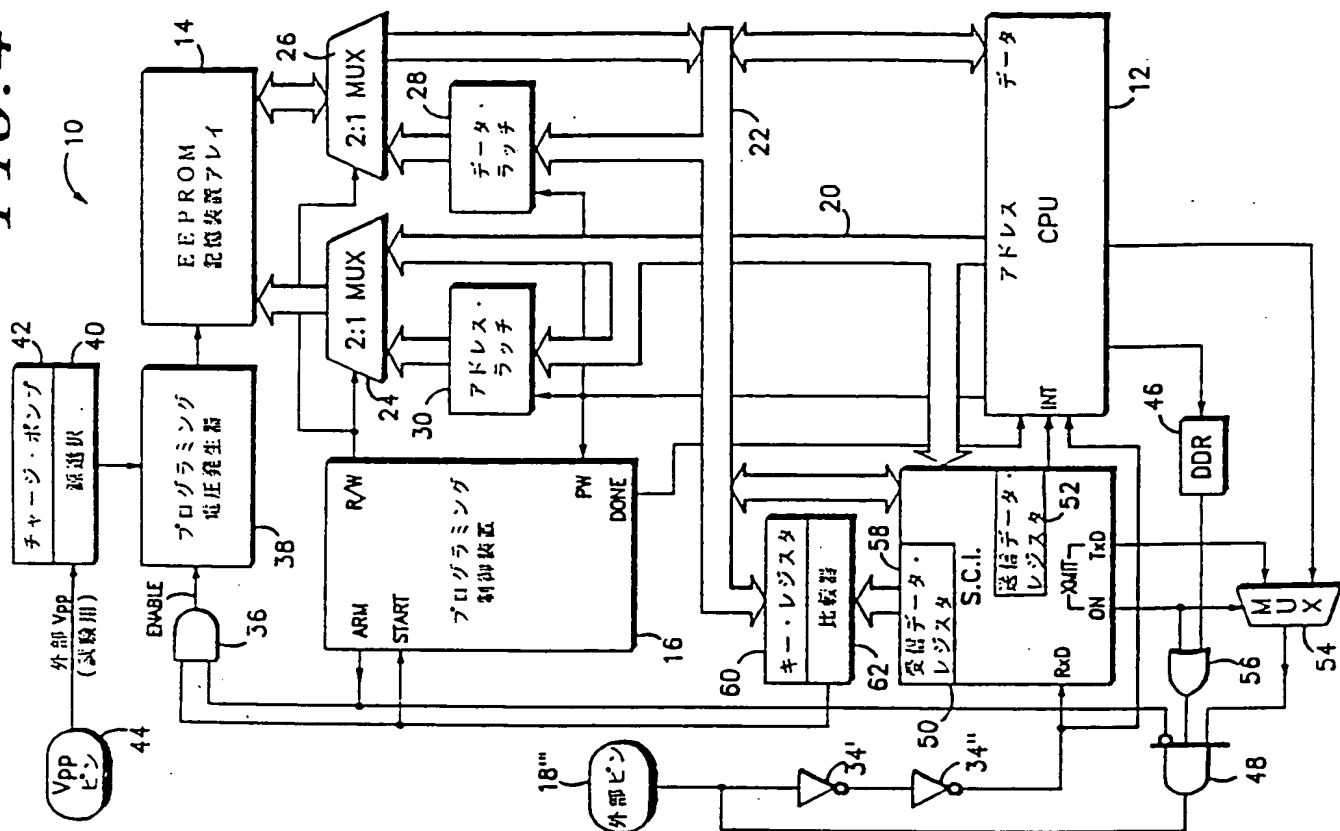


FIG. 5

